

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-011101

(43)Date of publication of application : 14.01.2000

(51)Int.Cl.

G06K 17/00
G06F 3/06
G06F 3/08
G06K 19/073
G06K 19/07

(21)Application number : 10-173163

(71)Applicant : HITACHI LTD

(22)Date of filing : 19.06.1998

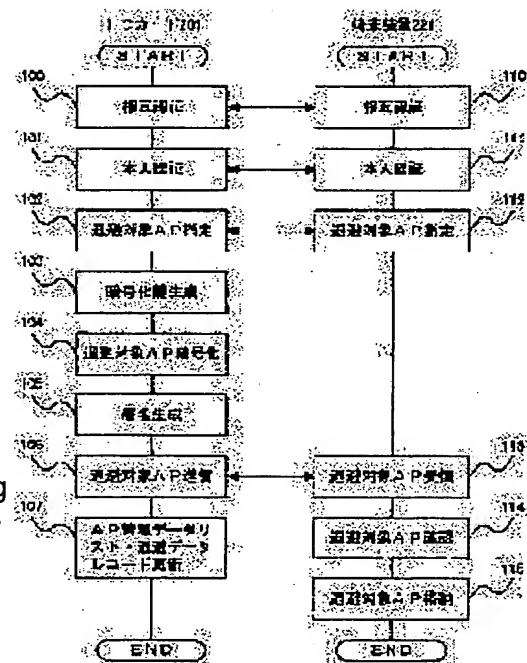
(72)Inventor : FUKUZAWA YASUKO
ORIMO MASAYUKI
HARAGUCHI MASATOSHI

(54) IC CARD AND RECORD MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To save an application program (AP) stored in an IC card according to the judgment of a user, and to prevent the illegal use of the saved AP.

SOLUTION: An IC card 201 generates and manages an arbitrary cryptographic key, and enciphers an AP to be saved among APS stored in an internal memory by using this cryptographic key, and saves this AP through an IC card reader/writer 211 to a connected terminal equipment 221, and deletes the AP before encipherment. Also, at the time of restoring the saved AP, the IC card 201 decodes the AP received from the terminal equipment 221 by using the managed cryptographic key, and restores the AP in the internal memory.



[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-11101

(P2000-11101A)

(43) 公開日 平成12年1月14日 (2000.1.14)

(51) Int.Cl. ⁷	識別記号	F I	テームコード* (参考)
G 0 6 K 17/00		G 0 6 K 17/00	B 5 B 0 3 5
			E 5 B 0 5 8
G 0 6 F 3/06	3 0 4	G 0 6 F 3/06	3 0 4 H 5 B 0 6 5
3/08		3/08	C
G 0 6 K 19/073		G 0 6 K 19/00	P

審査請求 未請求 請求項の数5 O L (全 10 頁) 最終頁に続く

(21) 出願番号 特願平10-173163

(22) 出願日 平成10年6月19日 (1998.6.19)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 福澤 寧子

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 織茂 昌之

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74) 代理人 100087170

弁理士 富田 和子

最終頁に続く

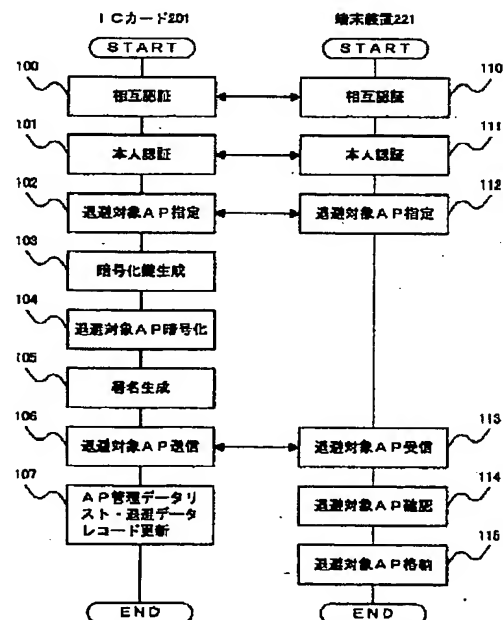
(54) 【発明の名称】 ICカードおよび記録媒体

(57) 【要約】

【課題】 ICカードに格納されているアプリケーションプログラム (AP) を、ユーザの判断で退避させることを可能とすると共に、退避させてあるAPの不正使用を防止する。

【解決手段】 ICカード201は、任意の暗号化鍵を生成して管理し、内部のメモリ202に格納されているAPのうちの、退避対象とするAPを、この暗号化鍵を用いて暗号化してから、ICカードリーダ/ライタ211を介して接続される端末装置221に退避させ、暗号化前のAPを消去する。また、ICカード201は、退避させておいたAPを回復させる際には、端末装置221から受け取ったAPを、管理しておいた暗号化鍵を用いて復号し、内部のメモリ202に再格納する。

図 1



【特許請求の範囲】

【請求項1】1つ以上のデータが内部のメモリに格納されているICカードであって、
退避対象とするデータの指定を外部から受け付ける手段と、

任意の暗号化鍵を生成する手段と、

退避対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを消去する手段と、

生成した暗号化鍵を記憶する手段と、

暗号化後のデータを外部に退避させる手段と、

退避させておいたデータを外部から受け取る手段と、

受け取ったデータを、記憶しておいた暗号化鍵を用いて復号する手段と、

復号後のデータを内部のメモリに再格納する手段とを備えたことを特徴とするICカード。

【請求項2】1つ以上のデータが内部のメモリに格納されているICカードであって、
無効化対象とするデータの指定を外部から受け付ける手段と、

任意の暗号化鍵を生成する手段と、

無効化対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを暗号化後のデータに置き換える手段と、

生成した暗号化鍵を記憶する手段と、

有効化対象とするデータの指定を外部から受け付ける手段と、

有効化対象として受け付けたデータを、記憶しておいた暗号化鍵を用いて復号する手段とを備えたことを特徴とするICカード。

【請求項3】請求項1または2記載のICカードであって、

内部のメモリに格納されている1つ以上のデータは、アプリケーションプログラムを含むことを特徴とするICカード。

【請求項4】請求項1記載のICカードがICカードリーダー/ライタを介して接続される端末装置にインストールされるプログラムを記録した記録媒体であって、

上記ICカードに格納されている1つ以上のデータのうちの、退避対象となるデータの指定を受け付けると共に、受け付けた指定内容を上記ICカードに出力する手段と、

上記ICカードから退避させられたデータを受け取って、上記端末装置のメモリに格納する手段と、

上記ICカードから退避させられて上記端末装置に格納されているデータのうちの、回復対象となるデータの指定を受け付ける手段と、

回復対象として受け付けたデータを上記ICカードに出力する手段とを、上記端末装置が備えるよう動作させるプログラムを記録したことを特徴とする記録媒体。

【請求項5】請求項2記載のICカードがICカードリーダー/ライタを介して接続される端末装置にインストールされるプログラムを記録した記録媒体であって、
上記ICカードに格納されている1つ以上のデータのうちの、無効化対象となるデータの指定を受け付けると共に、受け付けた指定内容を上記ICカードに出力する手段と、

上記ICカードに格納されているデータのうちの、有効化対象となるデータの指定を受け付けると共に、受け付けた指定内容を上記ICカードに出力する手段とを、上記端末装置が備えるよう動作させるプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、1つ以上のデータが格納されているICカードを運用管理する技術に係り、特に、セキュリティニーズに対する解決策を提示する技術に関するものである。

【0002】

【従来の技術】従来は、アプリケーションプログラム（以下、「AP」と称す。）が利用するデータのみをICカードに格納しておき、ICカードリーダー/ライタを介してこのデータを読み取った端末装置側で、APを動作させるようにした利用形態が一般的であった。

【0003】これに対し、近年、ICカード上でAPを動作させるための基本ソフト（カードOS）をICカードに格納することで、APをICカードに格納する動きが大きくなりつつある。

【0004】また、複数のAPを1枚のICカードに格納し、複数のICカードを1枚のICカードに統合することで、操作性を向上させ、ICカードのコストを、AP発行機関でシェアすることが期待されている。

【0005】なお、カードOSの一例としては、MULTOSが知られている。

【0006】MULTOSは、Fuji-Keizai USA「日米欧における電子アドバンス・カードのトレンドと今後のディレクション」という文献に記述がなされているように、ICカードに出力された様々なAPが、ICカードへのロードを正しく許可されたものか否かをチェックすると共に、個々のAPが、特殊なファイアウォール・プログラムによって分割して記録され、他のAPが動作を妨害しないことを保証している。ICカードへのロードが正しく許可されたものか否かをチェックするために、APのロードに先立って、管理機関は、APの正当性を検証し、正規利用者のICカードにのみロードされることを保証する処理を行う。ICカードにロードされたAPのデリートも、ロードと同様にチェックしてから行われるため、管理機関によって、該等するICカードからのデリートの正当性を保証する必要がある。

【0007】

【発明が解決しようとする課題】MULTOSは、管理機関の許可のないAPをICカードにロードすることができず、APがICカードに無制限にコピーされることを防ぐことができるので、有効な管理を実現することができることから、カードOSとして普及していきつつある。

【0008】しかしながら、このような厳密な管理は、ICカードの利用状況に応じて、ユーザの判断で、複数のAPが格納されたICカードから、特定のAPだけを一時的に退避させるような、フレキシブルな運用を制限してしまふ。

【0009】例えば、第三者が一時的にICカードを利用するときや、メモリ量の制約などから、しばらく必要としないAPをICカードから退避させ、使用したい他のAPと置き換えたい場合には、ユーザの判断で、ICカードに格納されているAPを退避させて無効化し、また、退避させておいたAPを回復させることが望まれる。

【0010】しかし、MULTOSをカードOSとしているICカードにおいては、上述したように、ICカードからのAPのデリート時にも管理機関の許可を必要とするので、ユーザの判断で、一時的にAPを退避させるような運用はできない。

【0011】本発明の目的は、ICカードに格納されているデータを、ユーザの判断で退避させることを可能とすると共に、退避させてあるデータの不正使用を防止することを可能とすることにある。

【0012】

【課題を解決するための手段】上記目的を達成するために、本発明は、ICカードに格納されているデータを、ICカード内で生成した暗号化鍵を用いてICカード内で暗号化し、暗号化後のデータをICカードから退避させるようにしている。また、生成した暗号化鍵をICカード内で管理しておき、退避させておいたデータを回復させる際には、このデータを、ICカード内で管理しておいた暗号化鍵を用いてICカード内で復号するようにしている。

【0013】すなわち、本発明は、第1の態様として、1つ以上のデータが内部のメモリに格納されているICカードであって、退避対象とするデータの指定を外部から受け付ける手段と、任意の暗号化鍵を生成する手段と、退避対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを消去する手段と、生成した暗号化鍵を記憶する手段と、暗号化後のデータを外部に退避させる手段と、退避させておいたデータを外部から受け取る手段と、受け取ったデータを、記憶しておいた暗号化鍵を用いて復号する手段と、復号後のデータを内部のメモリに再格納する手段とを備えたことを特徴としたICカードを提供している。

【0014】第1の態様によれば、ICカードから退避

させられたデータは、これを暗号化したICカード以外では復号できないので、不正使用されることがなくなる。

【0015】ここで、暗号化したデータをICカードから退避させる必要がない場合には、暗号化前のデータを暗号化後のデータに置き換えるようにすればよい。

【0016】すなわち、本発明は、第2の態様として、1つ以上のデータが内部のメモリに格納されているICカードであって、無効化対象とするデータの指定を外部から受け付ける手段と、任意の暗号化鍵を生成する手段と、無効化対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを暗号化後のデータに置き換える手段と、生成した暗号化鍵を記憶する手段と、有効化対象とするデータの指定を外部から受け付ける手段と、有効化対象として受け付けたデータを、記憶しておいた暗号化鍵を用いて復号する手段とを備えたことを特徴としたICカードを提供している。

【0017】なお、第1の態様および第2の態様のICカードいずれにおいても、内部のメモリに格納されている1つ以上のデータは、APを含むようにすることができるのは、当然である。

【0018】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【0019】図2は、本実施形態に係るICカードシステムの全体構成図である。

【0020】図2に示すように、本実施形態に係るICカードシステムは、ユーザが所有するICカード201と、端末装置221とが、ICカードリーダ/ライタ211を介して接続された構成となっている。

【0021】ICカード201は、MPU203と、メモリ202と、送受信IF204とを備えて構成され、端末装置221は、MPU223と、メモリ222と、キーボード224と、ディスプレイ225と、送受信IF226とを備えて構成されている。

【0022】また、ICカードリーダ/ライタ211は、送受信IF212と、送受信IF213とを備えて構成されている。

【0023】ICカード201および端末装置221は、ICカードリーダ/ライタ211を介して送受信を行うが、通信の形態は有線/無線を問わない。

【0024】次に、ICカード201のメモリ202に格納されている内容について、図3を用いて説明する。

【0025】図3に示すように、ICカード201のメモリ202には、例えば、クレジットやGSM(global system for mobile communication)等の、1つ以上APが格納されているが、ここでは、AP#1(321)およびAP#2(322)が格納されているものとす

る。

【0026】また、図3に示すように、ICカード201のメモリ202には、ICカード201ごとに固有の識別子であるカード識別子311と、非対称暗号における認証局の公開鍵312と、非対称暗号におけるICカード201の秘密鍵313と、非対称暗号におけるICカード201の公開鍵314と、AP管理情報315と、ICカード201へのアクセスを許可するためのパスワード316とが格納されている。

【0027】図7はAP管理情報315の一例を示す図である。

【0028】AP管理情報315は、ICカード201のメモリ202に格納されているAP（ここでは、AP#1（321）およびAP#2（322）である。）の各々に対応するAP管理データリスト700から構成されている。

【0029】図7に示すように、AP#1（321）のAP管理データリスト700は、AP#1（321）の識別子であるAP識別子701と、APファイル情報702と、AP#1（321）をICカード201へロードした回数を示すロードカウンタ703と、AP#1（321）をICカード201からデリートした回数を示すデリートカウンタ704と、図8に示す退避データレコード800へのポインタ705と、次のAPであるAP#2（322）のAP管理データリスト700へのエントリポインタ706とから構成されている。

【0030】なお、AP#2（322）のAP管理データリスト700も同様の構成である。

【0031】また、ポインタ705には、対応するAPを退避させていないならば、「NULL」が設定され、対応するAPを退避させているならば、退避データレコード800へのポインタが、APの退避が完了した時点で設定される。なお、退避データレコード800の詳細については後述する。

【0032】図3に戻って、ICカード201のメモリ202には、AP退避プログラム303と、AP回復プログラム304と、暗号化鍵生成プログラム305と、署名生成プログラム306と、対称暗号系暗号化／復号プログラム307と、非対称暗号系暗号化／復号プログラム308とが格納されている。

【0033】次に、端末装置221のメモリ222に格納されている内容について、図4を用いて説明する。

【0034】図4に示すように、端末装置221のメモリ222には、端末装置221ごとに固有の識別子である端末識別子411と、非対称暗号における認証局の公開鍵412とが格納されている。

【0035】また、図4に示すように、端末装置221のメモリ222には、AP退避プログラム403と、AP回復プログラム404と、署名検証プログラム405と、対称暗号系暗号化／復号プログラム406と、非対称暗号系暗号化／復号プログラム407とが格納されて

いる。

【0036】なお、ICカード201のメモリ202および端末装置221のメモリ222に格納される各種データは、各々、生成／発行／管理機関を設けることが考えられるが、ここでは、一般的に存在する認証局によって認証された公開鍵（認証局によって署名が施された公開鍵）を含む各種データが既に設定されているものとする。

【0037】次に、本実施形態に係るICカードシステムにおいて、ICカード201に格納されているAPを端末装置221に退避させる際の動作について、図1を用いて説明する。

【0038】図1は、本実施形態に係るICカードシステムにおけるAP退避時の動作の流れを示す図である。

【0039】端末装置221でAP退避プログラム403が起動され、ICカード201がICカードリーダ／ライタ211に挿入されると、ICカード201でAP退避プログラム303が起動され、以下の処理が実行される。なお、以下の処理は、ICカード201のMPU203および端末装置221のMPU223が、AP退避プログラム303およびAP退避プログラム403を実行することで実現される。

【0040】まず、ICカード201および端末装置221は、相互認証を行う（ステップ100、ステップ110）。相互認証については、例えば、ISO（ISO9798-3）に、非対称鍵暗号を用いた認証方式が規定されており、また、ISO（ISO9798-2）に、対称鍵暗号を用いた認証方式が規定されているので、ここでは詳細を省略する。

【0041】続いて、ICカード201および端末装置221は、本人認証を行う（ステップ101、ステップ111）。

【0042】本人認証においては、詳しくは、まず、端末装置221が、ディスプレイ225を介して、パスワードの入力をユーザに要求し、ユーザがキーボード224から入力したパスワードを、ICカード201に送信する（ステップ111）。

【0043】そして、ICカード201が、端末装置221からパスワードを受信すると、受信したパスワードとメモリ202に格納されているパスワード316とを比較し、正しいユーザであるか否かを認証する（ステップ101）。なお、ICカード201による認証結果は、端末装置221に通知される。

【0044】さて、正しいユーザであることが認証された場合は、ICカード201および端末装置221は、退避対象APの指定を行う（ステップ102、ステップ112）。

【0045】退避対象APの指定においては、詳しくは、まず、端末装置221が、ICカード201に格納されているAPの一覧を、ICカード201から取得し

でディスプレイ225に表示し、ユーザがキーボード224から指定したAPを、退避対象APとして、ICカード201に通知する(ステップ112)。なお、退避対象APの通知は、図5に示すAP指定データレコード500を送信することで行われる。

【0046】図5はAP指定データレコード500の一例を示す図である。

【0047】図5に示すように、AP指定データレコード500は、退避対象APを一意に指定するための識別子であるAP識別子501と、端末装置221の端末識別子(メモリ222に格納されている端末識別子411)502と、退避対象APの指定を端末装置221が受け付けた日時を示すタイムスタンプ503とから構成されている。

【0048】そして、ICカード201が、端末装置211からAP指定データレコード500を受信することで、退避対象APの指定を受け付ける(ステップ102)。

【0049】続いて、ICカード201は、AP指定データレコード500を受信すると、暗号化鍵生成プログラム305を起動することによって、退避対象APを暗号化するための暗号化鍵を生成する(ステップ103)。ここでは、退避対象APを対称暗号で暗号化するものとし、生成する暗号化鍵は、対称暗号における暗号化鍵(例えば、乱数)である。

【0050】続いて、ICカード201は、対称暗号系暗号化/復号プログラム308を起動することによって、ステップ103で生成した暗号化鍵を用いて、退避対象APを暗号化すると共に、暗号化前のAPを消去する(ステップ104)。

【0051】続いて、ICカード201は、署名生成プログラム306を起動することによって、署名を生成する(ステップ105)。

【0052】ステップ105では、詳しくは、ICカード201は、図9に示す署名生成用データレコード900から、ハッシュ関数を用いて認証子を生成し、非対称暗号系暗号化/復号プログラム308を起動することによって、メモリ202に格納されているICカード200の秘密鍵313を用いて、生成した認証子を暗号化して、署名を生成する。なお、ハッシュ関数および署名生成の詳細は、例えば、岡本龍明他著「現代暗号」、産経図書発行を参照されたい。

【0053】図9は署名生成用データレコード900の一例を示す図である。

【0054】図9に示すように、署名生成用データレコード900は、退避対象APのAP識別子901と、暗号化した退避対象AP902と、端末識別子(端末装置221から受信したAP指定データレコード500中の端末識別子502)903と、タイムスタンプ(端末装置221から受信したAP指定データレコード500中

のタイムスタンプ503)904と、ICカード201のカード識別子(メモリ202に格納されているカード識別子313)905とから構成されている。

【0055】続いて、ICカード201および端末装置211は、暗号化した退避対象APの送受信を行う(ステップ106、ステップ113)。

【0056】暗号化した退避対象APの送受信においては、詳しくは、まず、ICカード201が、暗号化した退避対象APを、端末装置221に送信する(ステップ106)。なお、暗号化した退避対象APの送信は、図6に示す退避APデータレコード600を送信することで行われる。

【0057】図6は退避APデータレコード600の一例を示す図である。

【0058】図6に示すように、退避APデータレコード600は、暗号化した退避対象APのAP識別子601と、ステップ104で暗号化した退避対象AP602と、ICカード201のカード識別子(メモリ202に格納されているカード識別子313)603と、ステップ105で生成した署名604と、ICカード201の公開鍵605(メモリ202に格納されている公開鍵314)とから構成されている。

【0059】そして、端末装置221が、ICカード201から退避APデータレコード600を受信することで、暗号化された退避対象APを受信する(ステップ113)。

【0060】さて、端末装置221は、退避APデータレコード600を受信すると、署名検証プログラム405を起動することによって、退避APデータレコード600中の署名604を検証する(ステップ114)。

【0061】ステップ114では、詳しくは、端末装置221は、非対称暗号系暗号化/復号プログラム407を起動することによって、まず、退避APデータレコード600中の公開鍵605を、認証局の公開鍵412を用いて復号して、公開鍵605を検証し、続いて、退避APデータレコード600中の署名604を、検証した公開鍵605を用いて復号して、署名604を検証する。

【0062】そして、端末装置221は、ステップ114による検証の結果、退避APデータレコード600がICカード201から送信されたものであること、および、退避APデータレコード600が改ざんされていないことを確認すると、退避APデータレコード600を、メモリ222またはディスク装置等に格納する(ステップ115)。なお、端末装置221は、APの退避に成功した旨をICカード201に通知する。

【0063】そこで、ICカード201は、APの退避に成功した旨が端末装置221から通知されると、対応するAP管理データリスト700を更新する(ステップ107)。

【0064】ステップ107では、具体的には、ICカード201は、退避データレコード800を生成し、生成した退避データレコード800へのポインタを、対応するAP管理データリスト700中のポインタ705に設定する。

【0065】図8は退避データレコード800の一例を示す図である。

【0066】図8に示すように、退避データレコード800は、端末識別子（端末装置221から受信したAP指定データレコード500中の端末識別子502）801と、タイムスタンプ（端末装置221から受信したAP指定データレコード500中のタイムスタンプ503）802と、ステップ103で生成した暗号化鍵803と、ステップ105で生成した署名804とから構成されている。

【0067】以上に説明した動作によって、ICカード201に格納されているAPを、端末装置221に退避させることができる。

【0068】なお、図1に示した動作においては、対称暗号で退避対象APを暗号化するようにしているが、非対称暗号で退避対象APを暗号化するようにしてもよい。この場合には、ICカード201は、ステップ103では、非対称暗号のアルゴリズムに応じた暗号化鍵を生成するようにする。

【0069】また、図1に示した動作において、ICカード201および端末装置221は、ステップ100およびステップ110の相互認証の過程で、一時鍵を共有することができるので、退避APデータレコード600を、この一時鍵を用いて暗号通信するようにしてもよい。

【0070】また、図1に示した動作において、端末装置221は、ユーザに退避場所を指定させるようにし、ユーザがキーボード224から指定した場所に、退避APデータレコード600を格納するようにしてもよい。

【0071】また、図1に示した動作においては、セキュリティ性をより高めるために、署名による認証技術を利用して、退避APデータレコード600がICカード201から送信されたものであること、および、退避APデータレコード600が改ざんされていないことを確認するようにしているが、これによって本発明の主旨が限定されることはない。

【0072】次に、本実施形態に係るICカードシステムにおいて、図1に示した動作で退避させたAPを回復させる際の動作について、図10を用いて説明する。

【0073】図10は、本実施形態に係るICカードシステムにおけるAP回復時の動作の流れを示す図である。

【0074】端末装置221でAP回復プログラム404が起動され、ICカード201がICカードリーダ/ライタ211に挿入されると、ICカード201でAP

回復プログラム304が起動され、以下の処理が実行される。なお、以下の処理は、ICカード201のMPU203および端末装置221のMPU223が、AP回復プログラム304およびAP回復プログラムを実行することで実現される。

【0075】まず、ICカード201および端末装置211は、図1で説明した動作と同様に、相互認証を行い（ステップ100、ステップ110）、本人認証を行う（ステップ101、ステップ111）。

【0076】そして、正しいユーザであることが認証された場合は、ICカード201および端末装置211は、回復対象APの指定を行う（ステップ1002、ステップ1012）。

【0077】回復対象APの指定においては、詳しくは、まず、端末装置221が、ICカード201に格納されているAPのうちの、退避中のAPの一覧を、ICカード201から取得してディスプレイ225に表示し、ユーザがキーボード224から指定したAPを、回復対象APとして、ICカード201に通知する（ステップ1012）。なお、回復対象APの通知は、退避対象APの通知と同様に、AP指定データレコード500を送信することで行われる。

【0078】そして、ICカード201が、端末装置211からAP指定データレコード500を受信することで、回復対象APの指定を受け付ける（ステップ1002）。

【0079】続いて、ICカード201は、AP指定データレコード500を受信すると、回復対象APのAP管理データリスト700、および、該AP管理データリスト700中のポインタ705が示す退避データレコード800を取り出す（ステップ1003）。

【0080】続いて、ICカード201および端末装置211は、回復対象APの送受信を行う（ステップ1004、ステップ1013）。

【0081】回復対象APの送受信においては、詳しくは、まず、端末装置211が、メモリ222またはディスク装置等に格納しておいた退避APデータレコード600を、回復対象APとして、端末装置221に送信する（ステップ1013）。そして、ICカード201が、端末装置211から退避APデータを受信することで、回復対象APを受信する（ステップ1004）。

【0082】さて、ICカード201は、退避APデータレコード600を受信すると、退避APデータレコード600中の署名604と、ステップ1003で取り出した退避データレコード800中の署名804とが一致するか否かを確認する（ステップ1005）。

【0083】そして、ICカード201は、両者が一致することを確認すると、対称暗号系暗号化/復号プログラム307を起動することによって、受信した退避APデータレコード600中の暗号化AP602を、ステッ

ブ1003で取り出した退避データレコード800中の暗号化鍵803を用いて復号し、復号した回復対象APを、ステップ1003で取り出したAP管理データリスト700中のファイル情報702に従って、メモリ202内に再配置する(ステップ1006)。

【0084】さらに、ICカード201は、回復対象APのAP管理データリスト700を更新する(ステップ1007)。

【0085】ステップ1007では、具体的には、ICカード201は、ステップ1003で取り出した退避データレコード800を消去し、回復対象APのAP管理データリスト700中のポインタ705に「NULL」を設定する。

【0086】以上に説明した動作によって、端末装置221に退避させておいたAPを、ICカード201に回復させることができる。

【0087】以上説明したように、本実施形態に係るICカードシステムによれば、ICカード201に格納されているAPを、ユーザの判断で、ICカード201から端末装置221に退避させることが可能になる。そして、退避対象APを、ICカード201内で生成した暗号化鍵を用いて暗号化するようにしているので、ICカード201から退避させられたAPは、これを暗号化したICカード201以外では復号できず、不正使用されることがない。

【0088】そこで、特に、ICカード201が、MULTOSをカードOSとしている場合でも、図1に示した動作を行うことで、ユーザの判断で、一時的にAPを退避させるようなフレキシブルな運用を実現することができる。

【0089】ところで、本実施形態に係るICカードシステムにおいては、ICカード201に格納されているAPを、端末装置221に退避させるようにしているが、ICカード201のメモリ202に余裕がある場合など、暗号化したAPをICカード201から退避させる必要がない場合には、APを退避させる代わりに、ICカード201内でAPを一時的に無効化するようにすることができる。

【0090】以下、このようにした場合の動作について、図11を用いて説明する。

【0091】図11は、本実施形態に係るICカードシステムにおけるAP無効化時の動作の流れを示す図である。

【0092】図11に示す動作は、図1に示した動作と同様であるが、ステップ1106において、ICカード201が、暗号化したAPを、ICカード201内に格納するようにした点が異なる。そこで、上述した各種データにおいて、退避/回復させるために必要であった部分には、何も設定されないこととなる。

【0093】図11に示した動作によれば、APを実際

には退避させていないが、ICカード201内でAPを暗号化しているので、第三者の脅威から護ることができる。

【0094】なお、無効化されたAPを有効化する際の動作は、ICカード201が、暗号化されて無効化されているAPを、これを暗号化したときに用いた暗号化鍵を用いて復号すればよい。

【0095】また、図11に示した動作を行うようにする場合には、端末装置221において、APを退避させるか、または、無効化させるかという選択を、ユーザに指定させるようにする必要がある。

【0096】また、図11に示した動作は、図1に示した動作とは独立に行うことが可能である。すなわち、図11に示した動作のみを行うICカードシステムを構築することが可能である。

【0097】なお、以上の説明では、退避対象および無効化対象とするデータがAPであるものとしているが、AP以外の他のデータであってもよいことは、説明するまでもない。

【0098】

【発明の効果】以上説明したように、本発明によれば、ICカードに格納されているデータを、ユーザの判断で、ICカードから退避させることが可能になる。そして、退避させるAPを、ICカード内で生成した暗号化鍵を用いて暗号化するようにしているので、ICカードから退避させられたデータは、これを暗号化したICカード以外では復号できず、不正使用されることがない。

【図面の簡単な説明】

【図1】本実施形態に係るICカードシステムにおけるAP退避時の動作の流れを示す説明図。

【図2】本発明の実施形態に係るICカードシステムの全体構成図。

【図3】本発明の実施形態におけるICカードのメモリに格納されている内容を示す説明図。

【図4】本発明の実施形態における端末装置のメモリに格納されている内容を示す説明図。

【図5】本発明の実施形態におけるAP指定データの一例を示す説明図。

【図6】本発明の実施形態における退避APデータの一例を示す説明図。

【図7】本発明の実施形態におけるAP管理情報の一例を示す説明図。

【図8】本発明の実施形態における退避データの一例を示す説明図。

【図9】本発明の実施形態における署名生成用データの一例を示す説明図。

【図10】本実施形態に係るICカードシステムにおけるAP回復時の動作の流れを示す説明図。

【図11】本実施形態に係るICカードシステムにおけるAP無効化時の動作の流れを示す説明図。

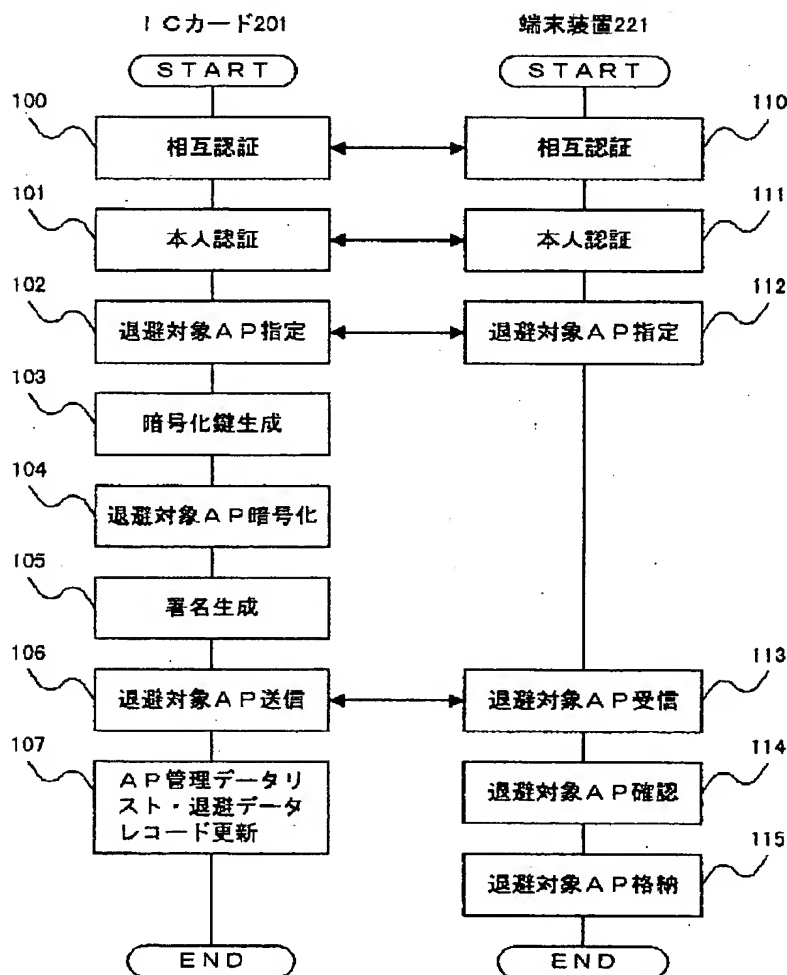
【符号の説明】

201…ICカード、211…ICカードリーダ/ライタ、221…端末装置、202、222…メモリ、203、223…MPU、204、212、213…送受信IF、224…キーボード、225…ディスプレイ、5*

*00…AP指定データレコード、600…退避APデータレコード、700…AP管理データリスト、800…退避データレコード、900…署名生成用データレコード。

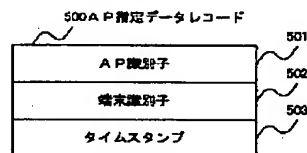
【図1】

図 1



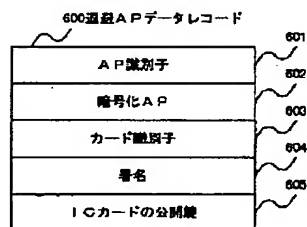
【図5】

図 5



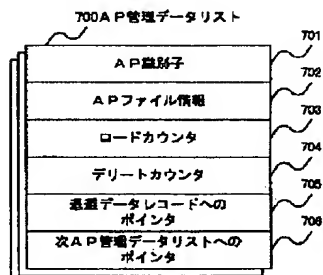
【図6】

図 6



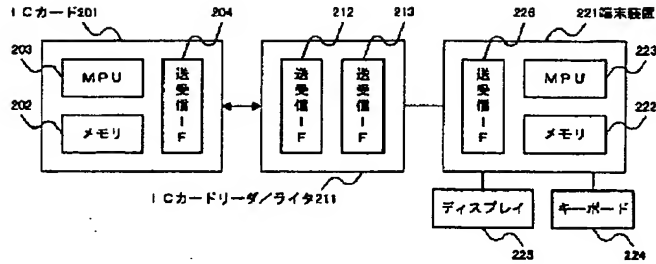
【図7】

図 7



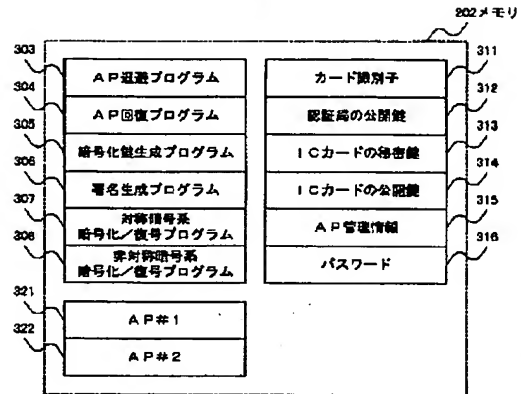
【図2】

図 2



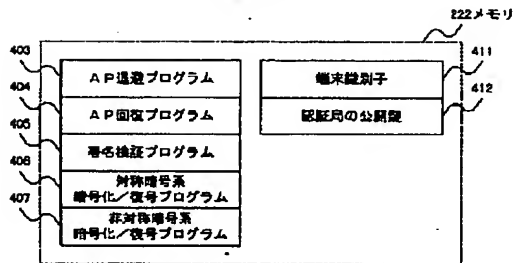
【図3】

図 3



【図4】

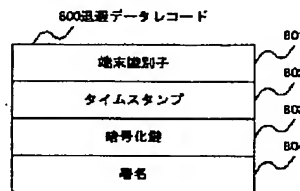
図 4



【図10】

【図8】

図 8



【図9】

図 9

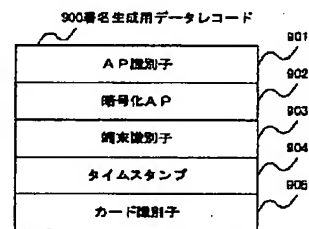
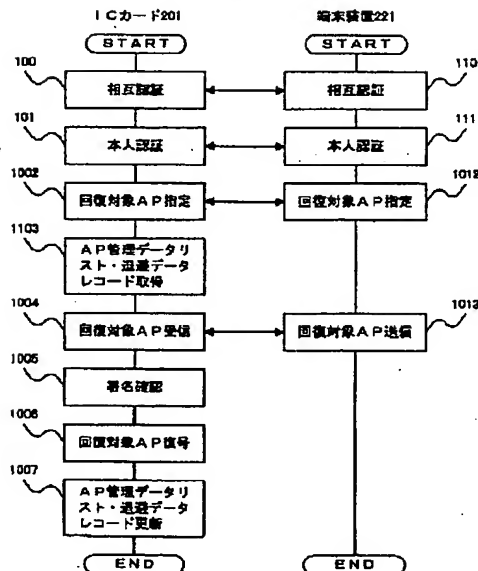
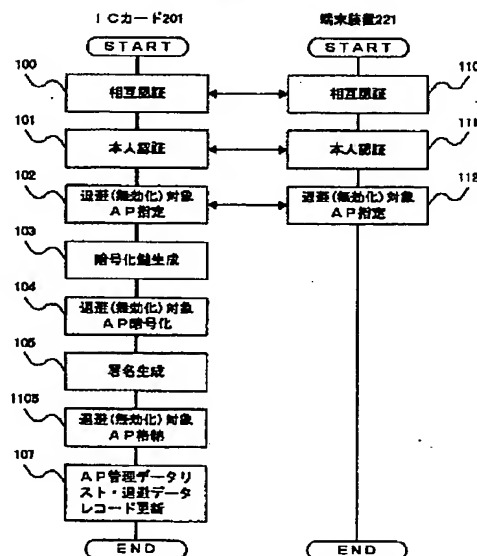


図 10



【図11】

図 11



フロントページの続き

(51)Int.Cl.

識別記号

F I

テーマコード(参考)

G 0 6 K 19/07

G 0 6 K 19/00

N

(72)発明者 原口 政敏

F ターム(参考) 5B035 AA13 8B09 BC03 CA29 CA38

神奈川県横浜市戸塚区戸塚町5030番地 株

5B058 CA27 KA01 KA04 KA35 YA13

式会社日立製作所ソフトウェア開発本部内

5B065 BA09 PA16